

Exhibit 64

**Excerpts of Harry Griffiths
Deposition Transcripts**

Harry Griffiths
9/30/2024

VIDEOTAPED DEPOSITION OF
HARRY GRIFFITHS
Austin, Texas
Monday, September 30, 2024

24 Reported by:
Micheal A. Johnson, RDR, CRR
25 Job No. 240930MJ

1

(3)

14 Videotaped deposition of HARRY GRIFFITHS,
15 taken on behalf of Plaintiff, at Latham & Watkins,
16 LLP, 300 Colorado Street, Suite 2400, Austin, Texas,
17 beginning at 10:09 a.m. and ending at 7:29 p.m. on
18 September 30, 2024, before Micheal A. Johnson, a
19 Registered Diplomatic Reporter, Certified Realtime
20 Reporter, and Notary Public of the State of Texas.

1 APPEARANCES:
2 ON BEHALF OF PLAINTIFF:
3 U.S. SECURITIES AND EXCHANGE COMMISSION
4 BY: Christopher J. Carney
Kristen M. Warden
Lory C. Stone (Via Zoom)
5 100 F Street, NE
Washington, D.C. 20549
6 (202) 256-7941
carneyc@sec.gov
7 wardenk@sec.gov
stonel@sec.gov
8
9 ON BEHALF OF DEFENDANTS
SOLAR WINDS CORP. AND TIMOTHY G. BROWN:
10 LATHAM & WATKINS LLP
11 BY: Serrin Turner
Joshua A. Katz
12 1271 Avenue of the Americas
New York, New York 10020
13 (212) 906-1330
serrin.turner@lw.com
josh.katz@lw.com
14
15 ALSO PRESENT:
16 Becky Melton
17 Jason Bliss
18
19 VIDEOGRAPHER:
20 Timothy Desadier
21
22
23
24
25

	INDEX
	HARRY GRIFFITHS
	September 30, 2024
	APPEARANCES 3
	PROCEEDINGS 8
	EXAMINATION OF HARRY GRIFFITHS:
	BY MR. CARNEY 9
	BY MR. TURNER 199
	BY MR. CARNEY 203
	REPORTER'S CERTIFICATION 205

2

4

Harry Griffiths
9/30/2024

<p>1 DEPOSITION EXHIBITS 2 HARRY GRIFFITHS 3 September 30, 2024</p> <p>4 EXHIBIT NO. DESCRIPTION MARKED</p> <p>5 Exhibit 1 April 8, 2020 E-mail, 51 Harry Griffiths to Jason Dee SW-SEC00416359</p> <p>6 Exhibit 2 May 3, 2019 E-mail, Harry 61 Griffiths to Sandra O'Connell, et al. SW-SEC00619016 - SW-SEC00619017</p> <p>7 Exhibit 3 November 7, 2017 E-mail, 64 Timothy Brown to Louise Butler, et al. SW-SEC00337101 - SW-SEC00337109</p> <p>8 Exhibit 4 February 21, 2019 E-mail, 91 Steven Colquitt to Harry Griffiths SW-SEC00619166 - SW-SEC00619177</p> <p>9 Exhibit 5 April 23, 2019 E-mail, 99 SolarWinds JIRA to Harry Griffiths SW-SEC00617272 - SW-SEC00617273</p> <p>10 Exhibit 6 July 22, 2020 E-mail, 112 Martin Gebauer to Harry Griffiths, et al. SW-SEC00395446 - SW-SEC00395455</p> <p>11 Exhibit 7 March 31, 2020 E-mail, 126 Roberto Borlain to Roberto Borlain, et al. SW-SEC00073646 - SW-SEC00073650</p>	<p>1 DEPOSITION EXHIBITS 2 HARRY GRIFFITHS 3 September 30, 2024</p> <p>4 EXHIBIT NO. DESCRIPTION MARKED</p> <p>5 Exhibit 17 11/2/2020-11/30/2020 193 Short Message Report SW-SEC00236723 - SW-SEC00236811</p> <p>6 Exhibit 18 Image From Bates 194 SW-SEC00236759</p>
<p>5</p>	<p>7</p> <p>1 Austin, Texas, Monday, September 30, 2024 2 10:09 a.m. - 7:29 p.m.</p> <p>3</p> <p>4 THE VIDEOGRAPHER: Here begins the 5 deposition of Harry Griffiths taking place at Latham 6 & Watkins at 300 Colorado Street, Austin, Texas in 7 the matter of Securities and Exchange Commission 8 versus SolarWinds Corporation, et al. The case 9 number is 23-cv-9518-PAE.</p> <p>10 Today's date is September 30th, 2024. 11 The time on video is 10:09 a.m. The videographer is 12 Timothy Desadier and the court reporter is Micheal 13 Johnson.</p> <p>14 Counsel, please identify yourselves 15 and state whom you represent.</p> <p>16 MR. CARNEY: Christopher Carney for 17 the Securities and Exchange Commission.</p> <p>18 MS. WARDEN: Kristen Warden for the 19 Securities and Exchange Commission.</p> <p>20 MR. TURNER: Serrin Turner, Latham & 21 Watkins for the deponent.</p> <p>22 MR. KATZ: Josh Katz, Latham & 23 Watkins, for the defendants.</p> <p>24 MS. MELTON: Becky Melton, VP legal 25 for SolarWinds.</p>

Harry Griffiths
9/30/2024

1 **Q.** And is April 1st, 2020, when you first
2 became a member of the security group at SolarWinds?
3 **A.** That's correct. I first became -- I
4 moved over from the customer support/technical
5 support team into the security engineering
6 department.
7 **Q.** So when you moved over in April of 2020,
8 what was your position then?
9 **A.** So incident response would have been my
10 primary focus when they brought me in. Because of
11 my background knowledge and working with customers,
12 reporting vulnerabilities against the products, this
13 was really the -- the main reason why I was going to
14 be moved into the security team to help with that
15 and the customer-facing aspect of response.
16 **Q.** And so when you say your primary focus
17 was incident response, what do you mean by that?
18 **A.** So when we say "incident response,"
19 there's two aspects. There's the cybersecurity
20 incidents that may be reported to us or there's
21 product security incidents that may be reported to
22 us. And we deal -- dealt with both at the time.
23 **Q.** And what is the difference between
24 cybersecurity incidents and product security
25 incidents?

17

1 **A.** So there is -- in the code base there's
2 various -- how do you say this? So there's
3 different types of cross-site scripting as well.
4 There's stored cross-site scripting, there's
5 indirect, there's -- it's -- sorry, struggling here.
6 Can I pick another example just to talk over? Had a
7 little brain fart there. So let's go for remote
8 code execution. That's probably the highest
9 impacting potential vulnerability that we would get.
10 Remote code execution allows you to send code to a
11 web application and run locally on the server that
12 is running the web application code and execute
13 code, which is not intended behavior. So it's a
14 weakness in the product that allows you to
15 potentially run -- execute code with -- depending on
16 the type -- elevated privileges, for example,
17 running as local system on the server.
18 **Q.** And so you've described that as a product
19 security incident. What makes it a security
20 vulnerability?
21 **A.** Could you rephrase the question for me,
22 please?
23 **Q.** Sure. Sure. I'm just wondering, you
24 described these potential vulnerabilities and you
25 just gave us an example where it can run the web

19

1 **A.** So the product security incidents is
2 really around the vulnerabilities that may exist in
3 the product that have been picked up by scanners or
4 external reporters or customers and reported in to
5 us that we work through with the various different
6 departments to triage, validate, and if found valid,
7 work on responsible disclosure where we would then
8 have a fix, you know, developed and issued out to
9 our customers for disclosure.
10 On the cybersecurity incident, they can
11 stem from many different areas. For example, there
12 could be some malware detected somewhere that has
13 been validated on a particular machine, or it could
14 be a phishing e-mail, something like this where
15 there's been a validated sort of detection, right,
16 where we try to validate through this process.
17 **Q.** Okay. So with respect to the
18 cybersecurity, you mentioned examples such as
19 malware and phishing. Is there a specific example
20 you can give of what would be a product security
21 incident?
22 **A.** Sure. So a customer may report that they
23 have a cross-site scripting issue in the web portion
24 of the product.
25 **Q.** And what is a cross-site scripting issue?

18

1 application code and execute code, which is not the
2 intended behavior. And I'm just wondering, what is
3 the security risk in that type of incident?
4 **A.** The security risk is -- for these ones
5 for the remote code execution, can be very high
6 security because it could allow -- especially for a
7 public web server, it could allow any actor to
8 leverage this weakness in the code and be able to
9 send traffic, you know, through the browser through
10 the security tools and gain access or run code on
11 the server locally. And from there he may be able
12 to laterally move or elevate his privileges to be
13 able to do a lot worse damage on the internal
14 infrastructure.
15 **Q.** And have you dealt with any remote code
16 execution incidents while you were at SolarWinds?
17 **A.** Yes.
18 **Q.** And how -- first of all, how many times
19 has that happened?
20 **A.** It would be a very small handful. I
21 can't give exact numbers.
22 MR. TURNER: Just testify to what you
23 remember.
24 **A.** Maybe two or three.
25

20

Harry Griffiths
9/30/2024

1 BY MR. CARNEY:

2 Q. Did you say GRG function?

3 A. GRC. Like a governance risk compliance
4 area of the security team.

5 Q. Thank you.

6 A. No problem.

7 MR. TURNER: Been going about an
8 hour, Chris. Want to take a break?

9 MR. CARNEY: We can take a break now
10 if you want.

11 MR. TURNER: Harry's a smoker.

12 THE VIDEOGRAPHER: Going off the
13 record. Time is 11:01.

14 (Recess taken from 11:01 a.m. to
15 11:22 a.m.)

16 THE VIDEOGRAPHER: Back on the
17 record. Time is 11:22.

18 BY MR. CARNEY:

19 Q. Mr. Griffiths, before we broke, you had
20 mentioned some instances when you were in your
21 technical support role and customers submitted to
22 you penetration testing that they had done on their
23 own. Do you recall that?

24 A. Yes.

25 Q. I'm wondering -- and you had also

41

1 A. I can't recall specific examples. There
2 was a lot. There was many over the period of time.

3 Q. So first of all, you said there were many
4 over a period of time. What period of time?

5 A. From -- even when I was in the support
6 team up until when I was no longer working on the
7 incident response team, which would have been when
8 I -- maybe one to two years ago, when I changed
9 roles into this cloud and threat and vulnerability
10 management role.

11 Q. Okay. And just -- just to clear the
12 record, so these customer reports of vulnerabilities
13 from pen testing that were validated, they would
14 have begun in 2012?

15 A. Prior to me joining the security team.
16 So 2019 maybe. Yeah.

17 Q. 2019. Okay. And when you say that there
18 were many instances, can you give me a rough number
19 of how many times this happened?

20 MR. TURNER: Objection to form.

21 A. No, because we had multiple products. So
22 this wasn't just single instances. This was any
23 customer who used any SolarWinds product might
24 report a vulnerability.

25

43

1 mentioned that you would sort of kick it over to the
2 engineering team to see whether those results could
3 be validated; is that correct?

4 A. That's correct.

5 Q. Do you recall any instances where the
6 customer's penetration results were sent over to the
7 engineer team and the results were validated?

8 A. Sorry, the question -- so when you say
9 results that could be -- a pen test might have
10 several. So when they're valid, it's possible that
11 there was only maybe one out of ten that were
12 validated. I can't recall where everything on that
13 report was validated.

14 On the other hand, they might be
15 reporting just one vulnerability and that may have
16 been reported -- validated.

17 Q. So to follow up on what you just said, do
18 you recall any instances where customers did their
19 own pen testing, identified a vulnerability, sent it
20 to you, you sent it over to the engineering team for
21 validation and they validated that there was,
22 indeed, a vulnerability?

23 A. Yes.

24 Q. And do you recall a specific example
25 where that happened?

42

1 BY MR. CARNEY:

2 Q. And do you know whether in every instance
3 when a customer reported a vulnerability that was
4 validated, was that vulnerability then corrected?

5 A. Yes. If it was a valid vulnerability
6 that had risk out there, then, yes, the standard
7 process would be to see if there was any kind of
8 mitigations that could be applied and to work on an
9 actual fix in the code and change that code and
10 release a security patch for customers.

11 Q. And so what you just described was the
12 standard process, right?

13 A. Standard process.

14 Q. And you mentioned that there were many of
15 these vulnerabilities that were validated that were
16 reported by customers. Do you know if that standard
17 process was followed for every single one of those
18 vulnerabilities?

19 A. To the best of my knowledge it was.

20 Q. And do you have an understanding as to
21 why customers were picking up vulnerabilities
22 through their pen testing that had not yet been
23 identified by SolarWinds' internal pen testing?

24 A. As I mentioned before, one of the reasons
25 that can happen is the false positives that -- we

44

Harry Griffiths
9/30/2024

1 may not have logged a ticket because when
2 engineering -- they already know when they see
3 something like that and they're able to give the
4 explanation so documenting that.

5 Q. So let me break that down a bit. Would a
6 false positive -- let me strike that.

7 Could a false positive reported by a
8 customer still be an example of a vulnerability that
9 is validated?

10 MR. TURNER: Objection to form.

11 A. When I say "validation," I kind of mean
12 through the triage process. So if we've identified
13 that it's a false positive, then somebody has read
14 through that code to find out that it's not
15 exploitable. So in that case, yeah, it's validated.

16 BY MR. CARNEY:

17 Q. And you mentioned the many instances
18 where customers reported vulnerabilities that were
19 validated.

20 Among those instances were there ones
21 where they were true positives?

22 A. That they were valid vulnerabilities
23 that -- a risk, bring some sort of risk, yes.

24 Q. And do you recall, of the many instances
25 where customers reported these vulnerabilities and

1 A. They're different people. I'd -- can you
2 rephrase the question to help me, please?

3 BY MR. CARNEY:

4 Q. Sure. You described how there's many
5 different plug-ins and scanners that can be used to
6 conduct pen testing; is that right?

7 A. Uh-huh.

8 Q. And sometimes because of those
9 differences, customers were able to uncover
10 vulnerabilities that SolarWinds had not uncovered;
11 is that right?

12 A. That's correct. Customers or security
13 researchers as well.

14 Q. And do you have an understanding as to
15 why SolarWinds did not have those pen testing
16 resources available itself?

17 MR. TURNER: Objection to form.

18 A. They're external different pen testers.
19 I don't quite follow the question because...

20 BY MR. CARNEY:

21 Q. And I'm just trying to understand from
22 a -- you know, as a nontechnical person, why the
23 products that the customers were using would pick up
24 on vulnerabilities that the products SolarWinds was
25 using did not.

45

47

1 they were validated, about what percentage turned
2 out to be actual risks?

3 A. I don't recall any figures.

4 Q. Okay. And in the instances where
5 customers reported a vulnerability and it was
6 validated as an actual risk, do you have an
7 understanding as to why the customer would have
8 identified that risk through its pen testing before
9 SolarWinds had?

10 A. As I kind of explained before in the pen
11 testing scene, using different types of scanners,
12 using different types of plug-ins for the same
13 scanner can expand what you uncover. Sometimes it's
14 like you -- there's just so many aspects with like,
15 you know, tens of thousands -- I'm just throwing out
16 numbers, of lines of code. So it's always possible
17 for anyone, whether they're in the security team,
18 the engineering team or customers or external pen
19 testers, to find different results and different
20 findings, that's common across the industry.

21 Q. Okay. And correct me if I'm wrong. So
22 is it, these customers had pen test resources
23 available to them that SolarWinds did not?

24 MR. TURNER: Objection to form and
25 foundation.

1 A. I'm still kind of confused about the
2 question.

3 Q. All right. Let me try to unpack it a
4 little. You mentioned that a customer might have a
5 scanner that SolarWinds did not have available; is
6 that right?

7 A. That's right, yeah.

8 Q. Okay. And that scanner could pick up on
9 vulnerabilities that the SolarWinds scanners did not
10 pick up on, right?

11 A. It's possible, yeah.

12 Q. And I guess as a layperson, I'm just
13 wondering, do you have an understanding why
14 SolarWinds didn't have scanners that would also pick
15 up on that vulnerability?

16 MR. TURNER: Are you asking him why
17 SolarWinds did not have every pen testing software
18 available on the market?

19 MR. CARNEY: No. No, not asking
20 that.

21 MR. TURNER: What is the question
22 exactly?

23 BY MR. CARNEY:

24 Q. So I'm asking you why -- the universe of
25 pen testing tools that SolarWinds had available, why

46

48

Harry Griffiths
9/30/2024

1 were they not enough to pick up the vulnerabilities
2 that the customers were picking up?
3 MR. TURNER: Object to foundation.
4 A. I'm still struggling with this particular
5 question. It's kind of confusing me. This is not
6 specific to SolarWinds. This is going to happen in
7 any software company out there because, you know,
8 product vulnerabilities are inevitable. There's
9 different languages, different codes. As I
10 mentioned, huge code bases that go way back. This
11 is why we run things like Bug Bounty programs, is
12 because, you know, there is very
13 specific -- security researchers are experts who are
14 known for one best -- they may apply different
15 techniques that is not shared, standard, and they
16 may be able to find similar vulnerabilities no
17 matter which vendor it is, if that makes sense.
18 So sometimes they have -- they get --
19 they work with a vendor, they find that they were
20 correct and validated, and on -- some way of maybe
21 manipulating the code, et cetera, and they could
22 apply that to SolarWinds. So it's kind of natural
23 for -- I guess it's kind of natural for just any
24 vendor is not going to be able to know everything
25 that the thousands and thousands of security

49

1 it's -- it's possible.
2 Q. Why do you say it's possible?
3 A. As I mentioned before, they could be
4 using a completely different product that has, you
5 know, patented or specific rules, scanning that only
6 their product has, you know, that's
7 different -- completely different to other tools.
8 As mentioned, there's so many of these tools out
9 there.
10 Q. Did you ever -- sorry, were you finished?
11 A. Yeah.
12 Q. Apologies. Did you ever express any
13 concerns about the resources available within
14 SolarWinds for pen testing?
15 A. I don't recall if I had any concerns.
16 Q. Do you recall anyone expressing to you
17 concerns about the resources available within
18 SolarWinds for pen testing?
19 A. Not that I can recall.
20 (Deposition Exhibit 1 marked for
21 identification.)
22 (Witness reviews document.)
23 BY MR. CARNEY:
24 Q. Mr. Griffiths, for the record, you've
25 been handed what's been marked as Exhibit 1, and

51

1 researchers, millions, I don't know, across the
2 world who are uncovering new vulnerabilities or
3 uncovering new ways to exploit vulnerabilities. And
4 that logic can be applied to different software and
5 platforms and stuff.
6 BY MR. CARNEY:
7 Q. Okay. Do you ever recall an instance
8 where a customer uncovered a valid vulnerability and
9 concerns were raised within SolarWinds as to why did
10 we not detect this ourselves?
11 A. It's fairly standard practice. This is
12 going to be common as, again, in any corporation
13 with product vulnerabilities. So you just always
14 learn -- try to do continuous improvements where you
15 can. And if you can apply things that will help
16 improve, your lesson's learned, shall we say, and
17 you know, the root cause analysis, then you can
18 help, you know, protect this.
19 Q. And I guess my question was -- but do you
20 recall any instances where a customer uncovered one
21 of these vulnerabilities and people inside
22 SolarWinds expressed concern that this is something
23 we should have uncovered ourselves with our own pen
24 testing?
25 A. I don't recall any specifics, but

50

1 this is an e-mail exchange from April of 2020 and it
2 has the Bates stamp SW-SEC00416359.
3 And I -- I handed you this exhibit just
4 because I sort of want to understand the training
5 that you've gone through briefly. So when is
6 it -- at the bottom, you -- do you know Jason Dee,
7 D-e-e?
8 A. Yeah.
9 Q. And who is he?
10 A. The colleague, I believe he was in
11 support, but then here he was a technical trainer at
12 this time in the academy team.
13 Q. And he's kind of trying to get some sort
14 of career advice from you. Is that a fair
15 assessment?
16 A. That's fair.
17 Q. And you mentioned at the top that you
18 went through the EC-Council exams. What's that?
19 A. Yeah. EC-Council is a professional
20 certification body revolving around security, and
21 you can go for their training and you can get the
22 certifications.
23 Q. And what certifications did you get
24 through the EC-Council exams?
25 A. So here was the Certified Ethical Hacker

52

Harry Griffiths
9/30/2024

Harry Griffiths
9/30/2024

<p>1 A. I mean, Active Directory by nature does 2 this by design. So when you create your password, 3 your password is protected with a key. So it's a 4 way of securing the actual password itself. And 5 this is, like, built into Active Directory, which is 6 what we use when we log on.</p> <p>7 Q. So what does it mean for a password to be 8 individually salted and hashed, though?</p> <p>9 MR. TURNER: You want a crash course 10 in cryptography, is that what you're asking for?</p> <p>11 MR. CARNEY: No. Just a brief 12 explanation.</p> <p>13 A. Individually meaning every account that's 14 created has this form of encryption.</p> <p>15 BY MR. CARNEY:</p> <p>16 Q. With respect to the second paragraph, 17 where it says: SolarWinds employees are granted a 18 limited set of default permissions to access company 19 resources, do you know if that policy applied to all 20 SolarWinds employees at the time that you switched 21 over to the security team in 2020?</p> <p>22 A. I believe so. When I was in support, I 23 didn't have that level of access.</p> <p>24 Q. You believe so. Do you know whether it 25 was actually enforced as to all employees at</p>	<p>1 access I actually needed for my role and it was 2 always going to be having my manager in there to say 3 this is approved.</p> <p>4 Q. And aside from your personal experience, 5 do you know if that policy was enforced across the 6 board at SolarWinds?</p> <p>7 A. Outside of the security team, right?</p> <p>8 Q. Yes.</p> <p>9 A. I don't think I would have had -- or 10 remember any specifics or -- outside security.</p> <p>11 Q. Okay. And then the last sentence says: 12 Approvals are managed by workflow tools that 13 maintain audit records of changes.</p> <p>14 Are you familiar with the workflow tools 15 that are described there?</p> <p>16 A. What comes to mind is the help desk 17 system that we were using.</p> <p>18 Q. And was that during a time when you were 19 in customer support?</p> <p>20 MR. TURNER: Object to form.</p> <p>21 BY MR. CARNEY:</p> <p>22 Q. Let me ask it this way. Did the help 23 desk system that you're describing that you say 24 relates to the workflow tools described in this 25 paragraph about authentication and authorization,</p>
<p>85</p> <p>1 SolarWinds?</p> <p>2 A. I can't speak for everyone. I can just 3 talk about my experiences as a support engineer and 4 my role before having access to -- a lot more 5 limited than when I had the administrator account 6 assigned to me.</p> <p>7 Q. And fair enough. And I appreciate your 8 experience. I'm just trying to understand if you 9 have knowledge about what was done across the 10 company, and if you do, that's great; if you don't, 11 that's also great.</p> <p>12 A. My understanding from hiring people, for 13 example, in the security team is that when they 14 join, they would be given a limited set, but then we 15 would request specific group access for them 16 depending on the role.</p> <p>17 Q. And the last two sentences say: Requests 18 for additional access follow a formal process that 19 involves a request and then approval from a data or 20 system owner, manager or other executives, as 21 defined by our security guidelines.</p> <p>22 I'm going to stop right there. Do you 23 know if that sentence was accurate as of the time 24 that you joined the security team?</p> <p>25 A. Yes. I recall not having the level of</p>	<p>87</p> <p>1 was that the system you were using when you were in 2 the technical support group?</p> <p>3 A. Every employee would use the help desk 4 system in place to make requests.</p> <p>5 Q. And was there an audit record of changes 6 in that system?</p> <p>7 A. The help desk system has a record of 8 that, yeah.</p> <p>9 Q. And then finally in this document, last 10 thing I want to ask you about is the Software 11 Development Lifecycle at the bottom of this page. 12 If you would please read those two paragraphs to 13 yourself. 14 (Witness reviews document.)</p> <p>15 A. Yeah.</p> <p>16 BY MR. CARNEY:</p> <p>17 Q. Okay. Mr. Griffiths, during your time at 18 SolarWinds, have you had any responsibility for 19 ensuring that SolarWinds followed the software 20 development lifecycle?</p> <p>21 A. No, that would not be in my 22 responsibilities.</p> <p>23 Q. Do you know whether at the time you 24 joined the security team in 2020 whether SolarWinds 25 was, in fact, following a secure development</p>

Harry Griffiths
9/30/2024

<p>1 engineering was ignoring your e-mails about RAFs?</p> <p>2 A. I don't recall that.</p> <p>3 Q. Did you -- can you explain what you were</p> <p>4 saying here in the message I just read?</p> <p>5 A. So the first sentence -- I believe this</p> <p>6 is referring to this new dashboard that I was</p> <p>7 creating and that's what I'm saying, is I'm creating</p> <p>8 this to also help the engineering teams have that</p> <p>9 same level of visibility into those specific tickets</p> <p>10 that we identify.</p> <p>11 The second part I'm saying but they don't</p> <p>12 act, read my e-mails. I'm obviously talking about</p> <p>13 something specific. I don't remember the who and</p> <p>14 what, but I'm referring to them obviously not coming</p> <p>15 back to me. I don't know the time period or any</p> <p>16 details behind that.</p> <p>17 Q. Thank you, sir. I'm going to -- I'm now</p> <p>18 going to hand you what's been marked as Exhibit 15.</p> <p>19 (Deposition Exhibit 15 marked for</p> <p>20 identification.)</p> <p>21 BY MR. CARNEY:</p> <p>22 Q. As with the other ones, you can take the</p> <p>23 time you need to read context, but I'm just going to</p> <p>24 ask you about some specific messages. But this is</p> <p>25 another short message report containing messages</p>	<p>1 First of all, do you recall this</p> <p>2 conversation with Mr. Fitzek?</p> <p>3 A. I do not.</p> <p>4 Q. Do you know what things that -- in</p> <p>5 engineering that he thought were broken; do you</p> <p>6 recall?</p> <p>7 A. No, I do not.</p> <p>8 Q. Do you recall there being an issue with</p> <p>9 senior people leaving?</p> <p>10 A. No, not at that time.</p> <p>11 Q. Sitting here today, do you have an</p> <p>12 understanding of what it means when he said:</p> <p>13 Currently there is no way we fix what is in JIRA in</p> <p>14 the next five years?</p> <p>15 A. I mean, JIRA's used, as I mentioned, for</p> <p>16 ticketing. So fix meaning that there's problems.</p> <p>17 So that could be any kind of bugs, and we have a lot</p> <p>18 of products, a lot of different things.</p> <p>19 Q. Okay. You mentioned bugs. Do you know</p> <p>20 if you were discussing bugs or whether you were</p> <p>21 discussing vulnerabilities in this conversation; do</p> <p>22 you recall?</p> <p>23 A. No, I don't recall.</p> <p>24 Q. If you look up above it at 11:41, you</p> <p>25 mention: Will prevent a lot of cases, and</p>
<p>181</p> <p>1 between Harry Griffiths and Ondrej Fitzek and this</p> <p>2 is from November 2nd, 2020, to November 30th, 2020,</p> <p>3 and it bears the -- first page bears the Bates stamp</p> <p>4 of SW-SEC00236824.</p> <p>5 And just once again, sir, just flipping</p> <p>6 quickly through this, does this appear to be a set</p> <p>7 of messages between you and Mr. Fitzek?</p> <p>8 A. Yes.</p> <p>9 Q. Okay. And who is Mr. Fitzek?</p> <p>10 A. Ondrej is -- he was an engineer. And as</p> <p>11 I mentioned before, the application security area of</p> <p>12 engineering, he would have been a sort of lead</p> <p>13 engineer at the time.</p> <p>14 Q. And if I could ask you, please, to turn</p> <p>15 to the page ending in 829. And I'm using the bottom</p> <p>16 Bates stamp. There's two sets of Bates labels on</p> <p>17 this.</p> <p>18 All right. And if you look at the</p> <p>19 conversation that takes place around noon on</p> <p>20 November 4th, 2020, Mr. Fitzek says: I talk like</p> <p>21 2-4h per week with management, but all things that</p> <p>22 are broken in engineering, not looking good. More</p> <p>23 senior people are leaving too. Currently there's no</p> <p>24 way we fix what is in JIRA in next five years.</p> <p>25 And you respond: Oh, no.</p>	<p>183</p> <p>1 simplifies support on what they need to know before</p> <p>2 advancing to support hackers.</p> <p>3 Q. Do you know what that means?</p> <p>4 A. I do not, so I'm going back to see if it</p> <p>5 helps.</p> <p>6 (Witness reviews document.)</p> <p>7 A. Okay. It says that -- secure Orion</p> <p>8 document. So that's -- ending on 828 referring to</p> <p>9 the secure Orion document that we were working on at</p> <p>10 the time.</p> <p>11 BY MR. CARNEY:</p> <p>12 Q. And what's the secure Orion document?</p> <p>13 A. It's a document to help customers</p> <p>14 implement recommendations of controls, security</p> <p>15 aspects of the products, you know, references to</p> <p>16 what firewall ports are required, you know, as we</p> <p>17 talked about earlier. And there was sort of -- I</p> <p>18 believe references to known issues or typical KBs</p> <p>19 that might get applied if a customer reported a</p> <p>20 particular issue. They might have a set of steps to</p> <p>21 implement to help protect their environment in the</p> <p>22 application.</p> <p>23 Q. And do you know why that document was</p> <p>24 created?</p> <p>25 A. I believe it's to aid customers in</p>

Harry Griffiths
9/30/2024

1 just haven't been re-looked at after, you know,
2 three months that we're talking about or longer.
3 BY MR. TURNER:
4 Q. And what --
5 A. And retested -- huh?
6 Q. What are some other possible reasons?
7 A. That the ticket when it was initially
8 created had some -- some level of analysis, but not
9 thorough enough to determine whether it was
10 exploitable. So they could be false positives
11 still.
12 Q. And what did you actually know at the
13 time about the issues that these tickets concerned?
14 MR. CARNEY: Objection, form.
15 A. I don't believe I knew much about the
16 actual details of these tickets. This was just me
17 identifying the statistics from a query from the
18 conditions that we talked about earlier.
19 BY MR. TURNER:
20 Q. And what did you know about whether the
21 issues the tickets concerned had actually been
22 validated; in other words, whether they were false
23 positives or not?
24 A. I didn't -- I don't believe I was digging
25 into these 127 vulnerability tickets to do that.

1 **Q.** And what did you know about whether the
2 issues had actually been resolved but the tickets
3 had simply not been closed?
4 **A.** I don't know if they had been resolved
5 and that they just haven't been closed.
6 **Q.** And you said at one point that looking
7 back at your younger self you have more context on
8 this conversation. Could you just explain that
9 further?
10 **A.** Yeah. For the reasons that we just kind
11 of talked about. I didn't even have that context
12 looking at it. And volume doesn't necessarily
13 reflect the true accuracy of the tickets like this,
14 still didn't have the validation that I was
15 referring to either, whether it's actually still an
16 issue or whether it was exploitable. These are just
17 raw figures that I'm pulling to communicate that
18 back to the engineering leaders' teams, yeah, to go
19 through the risk acceptance process and ideally look
20 into these tickets, and as they're doing that with
21 the hope that they might close them, they might
22 already, you know, be fixed.
23 MR. TURNER: No further questions.
24 MR. CARNEY: Very briefly.

1 actual details of the tickets.
2 Q. Okay.
3 MR. CARNEY: No further questions.
4 MR. TURNER: I have nothing further
5 from us.
6 THE VIDEOGRAPHER: This concludes
7 today's testimony of Harry Griffiths. Going off the
8 record. Time is 7:29.
9 (Deposition concluded at 7:29 p.m.)
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

Harry Griffiths
9/30/2024

1 REPORTER'S CERTIFICATION

2 I, Micheal A. Johnson, Registered Diplomate
3 Reporter and Notary Public in and for the State of
4 Texas, certify that on the 30th day of
5 September, 2024 I reported the Videotaped Deposition
6 of HARRY GRIFFITHS, after the witness had first been
7 duly cautioned and sworn to testify under oath; said
8 deposition was subsequently transcribed by me and
9 under my supervision and contains a full, true and
10 complete transcription of the proceedings had at
11 said time and place; and that reading and signing
12 was not requested.

13 I further certify that I am neither counsel
14 for nor related to any party in this cause and am
15 not financially interested in its outcome.

16 GIVEN UNDER MY HAND AND SEAL of office on
17 this 7th day of October, 2024.

18
19
20 MICHEAL A. JOHNSON, RDR, CRR
NCRA Registered Diplomate Reporter
NCRA Certified Realtime Reporter

21
22 Notary Public in and for the
State of Texas
My Commission Expires: 8/8/2028

23
24
25 205